CLAIMS

What is Claimed is:

1. A method for controlling access to digital information, comprising:

encrypting said digital information using a data encrypting key;

encrypting said data encrypting key using a key encrypting key and information derived from a location identity attribute that defines at least a specific geographic location; and

associating said encrypted data encrypting key with said encrypted digital information such that said encrypted digital information can be accessed only at said specific geographic location.

2. The method of Claim 1, wherein said location identity attribute further comprises at least a location value and a proximity value of said specific geographic location.

3. The method of Claim 2, wherein said location value corresponds to a location of an intended receiver of said digital information.

4. The method of Claim 2, wherein said location value further comprises at least one of a latitude, longitude, altitude and time dimension.

5. The method of Claim 2, wherein said location value further comprises a universal location that encompasses the entire earth.

6. The method of Claim 3, wherein said proximity value corresponds to a zone that encompasses said location.

7. The method of Claim 1, further comprising communicating said encrypted digital information to a receiver of said digital information disposed at said specific geographic location.

8. The method of Claim 1, further comprising identifying location of a receiver at which access to said digital information is sought.

9. The method of Claim 8, wherein said location identifying step further comprises recovering said location from a GPS receiver.

10. The method of Claim 1, wherein said information derived from said location identity attribute further comprises a location value and a shape parameter.

11. The method of Claim 1, further comprising:

decrypting said data encryption key using a key decrypting key and a location value; and

decrypting said digital information using said data encryption key.

12. The method of Claim 11, further comprising deriving said location value from a signal received by a GPS receiver and a shape parameter.

13. The method of Claim 1, wherein said digital information further comprises a secret key, and further comprising the step of distributing said secret key to an intended receiver.

14. The method of Claim 11, further comprising rendering unusable said encrypted digital information if said step of decrypting said encrypted digital information is attempted at other than said specific geographic location.

15. The method of Claim 11, further comprising rendering unusable said encrypted digital information if said step of decrypting said encrypted digital information is attempted without using said key decrypting key.

16. The method of Claim 1, further comprising routing said encrypted digital information to an intended receiver through at least one distributor.

17. The method of Claim 16, wherein said routing step further comprises adding a layer of encryption of said data encrypting key for said at least one distributor.

18. The method of Claim 1, further comprising generating said data encryption key using a pseudo-random number generator.

19. The method of Claim 18, wherein said step of generating said encryption key further comprises using GPS signals to partially seed said pseudo-random number generator.

20. The method of Claim 1, further comprising decrypting said encrypted data encrypting key, and re-encrypting said data encrypting key using at least one of a different location identity attribute and a different key encrypting key.

21. The method of Claim 1, further comprising providing a key table used to store a plurality of keys including said key encrypting key.

22. The method of Claim 21, further comprising associating said plurality of keys with respective providers of said digital information.

23. The method of Claim 21, further comprising administering management of said plurality of keys in said key table.

24. The method of Claim 23, wherein said administering step further comprises adding, changing or deleting any one of said plurality of keys in said key table.

25. The method of Claim 23, wherein said key table is located with a remote device, and said administering step further comprises adding, changing or deleting any one of said plurality of keys in said key table remotely.

26. The method of Claim 25, wherein said administering step further comprises including a signature when adding, changing or deleting any one of said plurality of secret keys in said key table.

27. The method of Claim 21, wherein said step of providing a key table further comprises storing keys used for signing data and validating signatures

28. An apparatus for controlling access to digital information, comprising:

a processor having memory adapted to store software instructions operable to cause said processor to perform the functions of:

encrypting said digital information using a data encrypting key;

encrypting said data encrypting key using a key encrypting key and information derived from a location identity attribute that defines at least a specific geographic location; and

associating said encrypted data encrypting key with said encrypted digital information such that said encrypted digital information can be accessed only at said specific geographic location.

29. The apparatus of Claim 28, wherein said location identity attribute comprises at least a location value and a proximity value of said specific geographic location.

30. The apparatus of Claim 29, wherein said location value corresponds to a location of an intended receiver of said digital information.

31. The apparatus of Claim 29, wherein said location value further comprises at least one of a latitude, longitude, altitude and time dimension.

32. The apparatus of Claim 29, wherein said proximity value corresponds to a zone that encompasses said location.

33. The apparatus of Claim 28, wherein said processor is further operable to communicate said encrypted digital information to a receiver of said digital information located at said specific geographic location.

34. The apparatus of Claim 28, wherein said processor is further operable to identify location of a receiver at which access to said digital information is sought.

35. The apparatus of Claim 28, further comprising a GPS receiver coupled to said processor.

36. The apparatus of Claim 28, wherein said information derived from said location identity attribute further comprises a location value and a shape parameter.

37. The apparatus of Claim 28, wherein said digital information further comprises a secret key, and said processor is further operable to distribute said secret key to an intended receiver located at said specific geographic location.

38. The apparatus of Claim 28, wherein said processor is further operable to route said encrypted digital information to an intended receiver through at least one distributor.

39. The apparatus of Claim 28, further comprising a pseudo-random number generator operatively coupled to said processor to generate said data encrypting key.

40. The apparatus of Claim 28, wherein said processor is further operable to decrypt said encrypted data encrypting key, and re-encrypt said data encrypting key using at least one of a different location identity attribute and a different key encrypting key.

41. The apparatus of Claim 28, wherein said memory further comprises a key table used to store a plurality of keys including said key encrypting key.

42. The apparatus of Claim 41, wherein ones of said plurality of keys are associated with respective providers of said digital information.

43. The apparatus of Claim 41, wherein processor is further operable to add, change or delete any one of said plurality of keys in said key table.

44. The method of Claim 41, wherein said processor is further operable to provide a signature for authentication of one of said plurality of keys.

45. An apparatus for receiving digital information, comprising:

a processor having memory adapted to store software instructions operable to cause said processor to perform the functions of:

receiving encrypted digital information and an encrypted data encrypting key;

decrypting said data encrypting key using a key decrypting key and a location identity attribute that defines a specific geographic location of said apparatus; and

decrypting said encrypted digital information using said decrypted data encrypting key.

46. The apparatus of Claim 45, wherein said function of decrypting said encrypted digital information further comprises rendering unusable said encrypted digital information if decryption is attempted at other than said specific geographic location.

47. The apparatus of Claim 45, further comprising a GPS receiver coupled to said processor.

48. The apparatus of Claim 45, wherein said processor is further operable to re-encrypt said data encrypting key using at least one of a different location identity attribute and a different key encrypting key.

49. The apparatus of Claim 45, wherein said memory further comprises a key table used to store a plurality of keys including said key decrypting key.

50. The apparatus of Claim 45, wherein ones of said plurality of keys are associated with respective providers of said digital information.